

CLAIMS

- Sub
a2
1. In a network connected to a printer and a registration server, a network registration protocol for registering the printer on the network, including the steps of:
- 5 installing a secret unique identifier in the printer and in a database of the registration server, before the printer is connected to the network; then, when the printer is connected to the network, authenticating the printer to the server by comparing the secret unique identifiers installed in said printer and said server, using a secure transmission over said network.
- 10
2. The network registration protocol according to claim 1, including the further step of holding said secret unique identifier in non-volatile memory in said printer, together with a public unique identifier.
- 15
3. The network registration protocol according to claim 2, including the further step of creating a public key together with its paired private key in said printer.
4. The network registration protocol according to claim 3, including the further step of, at said time the printer is connected to the network, transmitting the secret
- 20 unique identifier, the public unique identifier and the public key over the network to the registration server using said secure transmission.
5. The network registration protocol according to claim 4, including the further step of testing the received secret unique identifier and public unique identifier in the
- 25 remote registration server to verify the identity of the printer.
6. The network registration protocol according to claim 5, where said secure transmission comprises the further step of said printer obtaining said registration server's certificate, authenticating it with reference to a certificate authority, using a public key-

exchange key in said certificate to exchange a secret session key with the server, and then using said secret session key to encrypt said transmission.

7. The network registration protocol according to claim 6, including the further
5 step, in the event the printer's identity is verified, of creating and signing a certificate containing said printer's public unique identifier and public signature key, in said server; and storing the printer's certificate in a database for retrieval by third parties wishing to exchange data with the printer.

10 8. A network registration signal for transmission over a network from a printer to a remote registration server to register the printer with the server, where the signal is transmitted at the first occasion the printer is connected to the network, and includes:
a secret unique identifier and a public unique identifier retrieved from non-volatile
memory in the printer and a public key which is created, together with a paired secret
15 key, in the printer, so that upon receipt of the signal at the registration server the secret unique identifier and public unique identifier are tested to verify the identity of the printer and, in the event the printer's identity is verified, a certificate is created and signed which contains the printer's public unique identifier and public signature key.